A THEOREM ON FACTORIZATION*

BY D. N. LEHMER

In a note in this Bulletin† I observed that if $R=pq$ is the product of two odd factors whose difference is less than twice the fourth root of R then the factors of R are obtainable directly from the expansion of $R^{1/2}$ in a continued fraction. This theorem comes from the fact that in view of a theorem due to Lagrange, $(p-q)^2/4$ will appear as a denominator of a complete quotient in that expansion, and that therefore the diophantine equation $x^2-Ry^2=(p-q)^2/4$ will have the integral solution $x=\frac{1}{2}(r+q)$, $y=1$.

The object of the present note is to point out that the method is of much wider application than the above statement would indicate. For consider the identity

$$\left(\frac{mp+nq}{2}\right)^2-\left(\frac{mp-nq}{2}\right)^2=mnpq.$$

From this it appears that if mn is a square and if m and n are both odd or both even, we will have an integral solution of the equation

$$x^2-Ry^2=\frac{1}{4}(mp-nq)^2,$$

namely

$$x=\frac{1}{2}(mp+nq),\qquad y=(mn)^{1/2}.$$

By Lagrange's theorem, therefore, if $mp-nq<2R^{1/4}$ one of the denominators in the expansion of $R^{1/2}$ will certainly be $(mp-nq)^2/4$ and since the numerator of the preceding convergent will be $(mp+nq)/2$ these two numbers will serve to furnish the factors p and q of R. We have then the following theorem.

* Presented to the Society, San Francisco Section, October 30, 1926.

† Vol. 13 (1906-7), p. 501. Translated in Sphinx-Oedipe, 1911. Given also in Kraitchik's *Recherches sur la Théorie des Nombres*, p. 73.

THEOREM. *If $R=pq$ is the product of two odd factors, and if two numbers m and n, both even or both odd, are obtainable such that their product is a square and also such that $mp-nq<2R^{1/4}$ then the continued fraction for $R^{1/2}$ will furnish without trial the factors p and q of R.*

It should be noted that if the difference $mp-nq$ is less than the fourth root of R the restriction that m and n be both even or both odd may be disregarded, for in that case $2m$ and $2n$ are suitable multipliers. Also it is worth noting that the square denominator will appear in the complete quotient when the denominator of the preceding convergent is $(mn)^{1/2}$. This means that in the original theorem the desired square is under the third complete quotient.

An example will indicate the method of attacking a number by this method. Let $A=1564{,}08789$. The square root expansion gives the following series of denominators for the complete quotients: 1, 8753, 15013, 3740, 529, $\cdots$, the partial quotients being 12506, 2, 1, 6, 47, $\cdots$. The convergent preceding the complete quotient with the square denominator 529 is found to be 250127/20. We have then

$$(mp+nq)/2 = 250127, \qquad (mp-nq)/2 = 23.$$

Whence

$$mp = 250150, \qquad nq = 250104.$$

Since, now, $pq=A$ and $mn=20^2=400$ it is easily found that $p=31263$, $q=5003$, $m=8$, $n=50$. The success of the method was due to the fact that the difference $mp-nq=46$, which is less that $2A^{1/4}=222$. In this example also we see that $36p-225q=207$, which is also less than 222; but since here the values of m and n differ in parity, these values will not appear in the expansion. Similarly the difference $mp-nq=23$ for $m=4$, $n=25$, and m and n being different in parity these values will also not appear in the expansion. But since 23 is less than $A^{1/4}$, we will have $2m$ and $2n$ for suitable values, and these are indeed the ones that do appear.

THE UNIVERSITY OF CALIFORNIA